UCRL-WEB-201520

File Interchange Service (FIS) Manual

Table of Contents

Preface

Scope: The File Interchange Service (FIS) Manual explains how to use tape transfers between two dedicated FTP nodes to move files between the open and the secure LC computing networks. Password requirements and levels of authorization for transferring files from the secure to the open side are described in detail. Examples show the directory structure used on each FTP node and the steps in the transfer process. For Authorized Derivative Classifiers (ADCs) approving secure-to-open transfers, explicit instructions are included for the FIS-assisting ADCTOOL as well as for LC's enhanced file-review utility called MOLE.

Availability: FIS is available to transfer binary or text files from open to secure machines. Secure-to-open transfers become available to each LLNL directorate as it repopulates its own ADC review pool and revises its transfer policy to meet current security requirements.

Consultant: For help contact the LC customer service and support hotline at 925-422-4531 (open e-mail: lc-hotline@llnl.gov, SCF e-mail: lc-hotline@pop.llnl.gov). A matrix showing related LC documentation arranged by subject and complexity level appears in the first section of DOCGUIDE (URL: http://www.llnl.gov/LCdocs/docguide).

Printing: The print file for this document can be found at:

```
on the OCF: http://www.llnl.gov/LCdocs/fis/fis.pdf
on the SCF: https://lc.llnl.gov/LCdocs/fis/fis_scf.pdf
```

Introduction

FIS is Livermore Computing's file interchange service, an operator-assisted way for LC users to transfer files between the Open (Unclassified) Computing Environment and the Secure (Classified) Computing Environment. This service is bidirectional and the mechanism used for transfer (tapes) is the same in both directions. But the user interface and operational aspects are different for secure-to-open transfers than for open-to-secure transfers. The difference reflects the asymmetric need to verify that only unclassified content moves from the secure to the open network, a need met by having your organization's Authorized Derivative Classifier(s) inspect the transferred files.

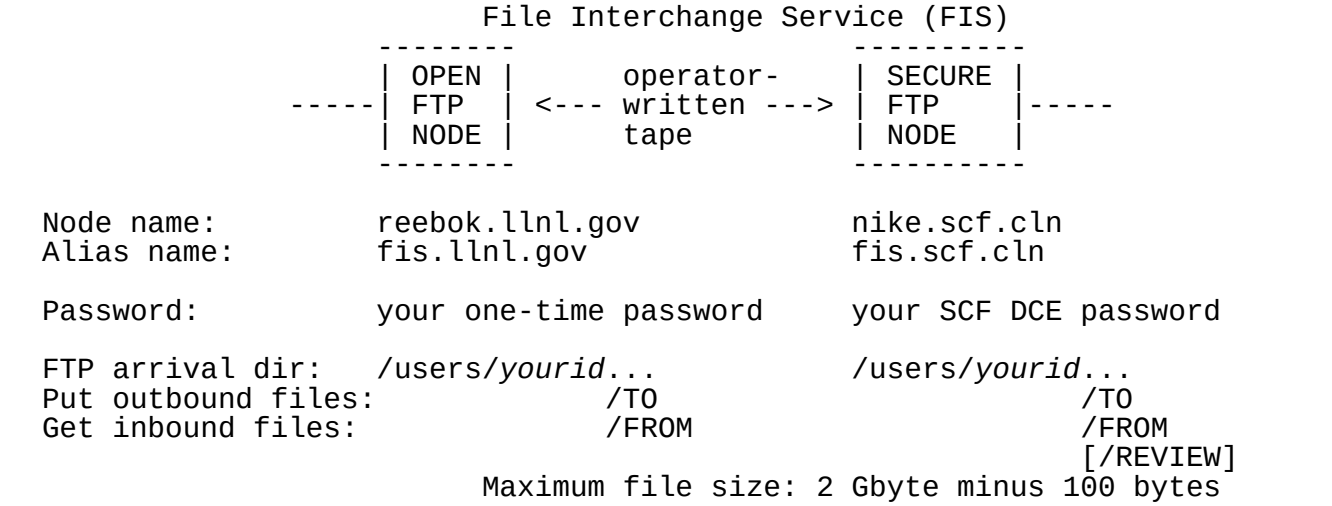
This document tells how FIS works and how to use it effectively. It also discusses the classification review categories that affect how you are authorized to transfer files from the secure to the open networks. For ADCs, instructions are included for using the FIS-assisting ADCTOOL to manage secure-to-open file reviews and for using LC's enhanced file-review utility called MOLE.

See the EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput) guide for a concise summary of the basic instructions for using FIS, as well as for help with general problems (for example, posed by Macintosh file formats and file names) associated with all between-machine file transfers. For help with technical details of FTP or SFTP, the only tools that interact with FIS, consult LC's FTP Reference Manual (URL: http://www.llnl.gov/LCdocs/ftp).

Overview of FIS Features

FIS (formerly called Hermes) consists of two transfer nodes, one on each environment. For the user, the transfer node represents the place to submit files for transfer and the place to retrieve files that have been transferred. For this service, these nodes possess the necessary tape resources to perform the transfer between environments. The preferred alias for the OCF transfer node is fis.llnl.gov (134.9.1.71) and the preferred alias on SCF is fis.scf.cln (130.106.230.9). Although the actual FIS node names appear below (and in FTP dialog), there is no need to learn or use them.

PROCESS:
This diagram summarizes the between-network file-interchange process:



The only access provided to a user of this service is via FTP (or, for OCF machines, SFTP). To protect security, usage of the transfer node is limited to this service and general login capability is disabled. To connect to a transfer node, an FTP client must be executable on your local machine.

WARNINGS:

(1) FTP ONLY: FIS has no interface to support secure copy (SCP), so that you cannot use SCP to deposit files on FIS or retrieve transferred files from FIS. You also cannot use NFT. On OCF machines only, you can encrypt the files that you send to the open FIS node by using "secure FTP" (SFTP), which behaves much like standard FTP but offers far fewer control options. SFTP is not available on SCF. For a comparison of SFTP with stardard FTP clients, see LC's .

(2) FIREWALL: LC now uses its hardware/software security "firewall" to block direct FTP connections from machines outside the llnl.gov domain to LC machines within llnl.gov (including FIS). Such FTP blocking means that you must start your FTP client on a within-llnl.gov machine (or one with a VPN virtual llnl.gov address). See the EZACCESS (URL: http://www.llnl.gov/LCdocs/ezaccess) basic introduction or the Firewall and SSH Guide (URL: http://www.llnl.gov/LCdocs/firewall) for more background on these access restrictions and ways to compensate for them.

(3) CONNECTIONS: The maximum number of simultaneous FTP connections to FIS is 25 (with SFTP, no maximum). While often an invisible limit, this may prevent your reaching the FIS node during busy file-exchange periods.

(4) NAMES: FIS automatically changes some characters in a file's name (not body) during transfer. See the subsection below (page 12) on "How FIS Handles File Names" for details and a work-around.

(5) CAPACITY: In August, 2002, the *total* capacity of the disks on both the open and secure FIS nodes was expanded to 36 Gbyte, to enable the simultaneous exchange of many large files. But the *per-file* FIS size limit remains at just under 2 Gbyte.

(6) TWO-PERSON RULE: DOE/LLNL information security rules now require that *two* people perform and witness all open-to-secure FIS transfers. During the work week, a pair of LC operators handles this. On weekends and holidays, however, only one operator is usually available so the two-person requirement cannot be met and no FIS transfers occur routinely. But if you need a weekend FIS transfer and you are on site, you can telephone the LC operations office (x24531) and then walk down to B-113 to serve as the "second person" yourself.

FIS Passwords and Authorization Requests

Requesting FIS Authorization

To use the file-interchange service (FIS) you must already have an account and valid password for at least one open and one secure machine. You then complete authorization form SCF-6 (available from the LC Hotline) and return it to the Hotline with an account number to be charged for each transfer.

Any user can receive authorization to move files from the open to the secure network. To receive authorization to move files from the secure to the open network you must specify the kinds of files to be moved and obtain the approval of your division leader or department head (in the appropriate places on the form). The instructions on the form remind you of these requirements in relation to each blank.

Once you are authorized, you will be able to use your current authenticator-generated one-time password (OTP, the same password process used for any open cluster) to access the open FIS node. On the secure side, the FIS node uses your secure DCE password (the password for White or the SCF Linux clusters, for example).

Password Policies

Each user of this service has an account on both transfer machines. A prerequisite for this is an established user record for LC's Secure Computing Facility (SCF). The user name for each account on each transfer machine is the same as that on any DCE machine (such as White or the Linux clusters) on the same network, so that you use your open DCE name on the open FIS node and your secure DCE name on the secure FIS node.

OPEN.
A special process for obtaining a unique open FIS password is no longer needed. Simply use your current authenticator-generated one-time password (OTP, the same as you would for any open computing cluster) when FTP (or SFTP) prompts for a password for the open FIS node. Hence FIS users should no longer ever need to voluntarily change a working open DCE password, by using a WWW browser on the open network and going to the URL

```
https://lc.llnl.gov/bin/passwd
```

(details of this process appear in the EZACCESS (URL: http://www.llnl.gov/LCdocs/ezaccess) guide). SFTP users can arrange to authenticate with "DSA keys" instead of with one-time passwords through a fairly elaborate set-up process. See the SFTP section of LC's FTP Reference Manual (URL: http://www.llnl.gov/LCdocs/ftp).

SECURE.

On the secure network, FIS no longer uses Kerberos authentication. Instead, simply use your current secure DCE password (the password for White or the SCF Linus clusters) when FTP prompts for a password for the secure FIS node. To voluntarily change a working secure DCE password, use a WWW browser on the SCF network and go to the URL

```
https://lc.llnl.gov/bin/passwd
```

(details of this process appear in the EZACCESS (URL: http://www.llnl.gov/LCdocs/ezaccess) guide).

Authorization Levels: The Classification Review Categories

The previous fourfold classification review categories (ADMIN, DUSA, NEED, and DENY) have been collapsed into just two exclusive categories (NEED and DENY). They define your ability and your mechanism for transferring unclassified files from the secure to the open network.

DENY Category

If you are a user with a review category of DENY, unfortunately, you are prohibited from transferring any data from the Secure Environment to the Open Environment. Your use of the secure transfer node is limited to retrieving files transferred from the Open Environment. You have a TO directory as part of the standard work space but you do not have write access for that directory.

NEED Category

If you are a user with a review category of NEED, you have the standard work space, TO and FROM directories, for submitting and retrieving files. Files that you place in the TO directory will be held in the TO directory awaiting ADC review and approval. Typically, you submit files into the TO directory and then seek out an ADC within your organization that is capable of reviewing your data. Your completed user request form contains the name of an ADC pool; the ADCs assigned to this pool are capable of reviewing your data. Ask your computer coordinator for the names of the ADCs assigned to this pool. Each department or division determines the elaborateness of its own file review policy for its own ADCs. Livermore Computing, for example, expects a "cognizant system administrator" ADC to review system data before a second, routine review by an "FIS ADC" takes place.

You and your ADC(s) would normally begin by discussing the content of your submitted files. The ADC is also able to select your files for review and examine them on his or her local computer (assisted by a special program called ADCTOOL (page 18)). The ADC can accept them as unclassified data and release them back into the transfer path or the ADC can reject them (because they are classified data) and purge the disk files.

When a file is selected for review by an ADC it is moved from your TO directory into a review area which is inaccessible by the user. (The former use of "permits" and "permit directories" to mitigate some file reviews has been eliminated to enhance security.) Now, all files should be submitted in the TO directory, where they await ADC inspection. As noted above, files that are held for review are removed from the user's TO directory and placed in a private review area accessible by only the ADC.

So how does one find out his or her files have completed review? One way is to ask the ADC; another is to look at the README file found in your top-level directory on the secure FIS node (/users/*yourname*/README). Each time a file has been reviewed (pass or fail) an entry is added to README; you can examine the tail end of this file for the results of the review or simply examine the modification time of the README file to determine if the review action has occurred.

DUSA Category

Use of the former DUSA (Designated Unclassified Subject Area) review category has been suspended.

ADMIN Category

Use of the former ADMIN (Administrative Information) review category has been suspended.

How to Use FIS

All users of this service are permitted to transfer from the Open Environment to the Secure Environment. It is the responsibility of each user to be mindful of the data he or she transfers and to safeguard against viruses, worms, trojan horses and other hazards. On both transfer machines, each user has a private work space. The work space on the OCF FIS node consists of two subdirectories, a TO and a FROM directory. The TO directory is where a user places files that he or she wishes to transfer to the Secure Environment. The user would retrieve transferred files from the FROM directory; these are files that have been transferred from the Secure Environment.

The work space on the SCF FIS node is basically the same as on the open FIS node (since only the DENY and NEED review categories are in use now). However, each secure user who tries to transfer files to the Open Environment also has a top-level README file (/users/*yourname*/README) to which messages about approved or disapproved secure-to-open transfers are appended each time an ADC review occurs.

We only describe the procedure for a transfer from the Open Environment to the Secure Environment. The transfer in the other direction follows the same pattern but requires ADC review (page 17) before files are actually copied to tape for transfer.

How FIS Handles File Names

When FIS moves files from one transfer node to another, it automatically changes some characters in each file name (*not* in the body of the file, just in the file name) to avoid characters troublesome to some UNIX file-handling utilities. This chart shows which file-name characters FIS changes during a transfer:

File-name Character:	FIS Changes To:
alphabetic	no change
numeric	no change
internal . (dot)	no change
leading . (dot)	_ (underscore)
ALL others (includes space, hyphen, quote)	_ (underscore)

For example, if you submit to the open-network FIS node a file called

```
.t-e+s$t.n"ame3
```

you will receive on the secure-network FIS node a file called

```
_t_e_s_t.n_ame3
```

Your own file-handling scripts and commands need to take account of these changes in file-name characters (on the receiving side) to avoid loosing or omitting some FIS-transferred files.

To preserve the special characters in a file's name unchanged, use the UNIX TAR utility to embed the file inside a TAR output file, transfer the TAR file in binary mode with FTP to FIS, then run TAR again on the receiving side to extract the original file with its original name.

Depositing Open-to-Secure Files

WARNINGS:

(1) FIS does not accept file transfers using secure copy (SCP) or NFT; you must use FTP (or "secure FTP," called SFTP (page 5)) as decribed here.

(2) If your files are not already on an llnl.gov machine, then the firewall warnings at the end of the Overview (page 5) section apply to you and you must run FTP on an llnl.gov machine to first get your files from outside.

(3) Files with blanks (spaces) or nonASCII characters in their names (such as some Macintosh files) will not be handled properly on UNIX machines, including both nodes of FIS. See the "Macintosh File-Transfer Problems" section of EZOUTPUT (URL: http://www.llnl.gov/LCdocs/ezoutput) for tips on preprocessing these special-name and special-format files BEFORE you send them to FIS. Also see the previous subsection (page 12) on how FIS handles all file names.

(4) The maximum number of simultaneous FTP connections with FIS is 25 (this could prevent reaching FIS during busy file-exchange periods). SFTP connections have no maximum.

(5) DOE/LLNL information security rules now require that *two* people perform and witness all open-to-secure FIS transfers. During the work week, a pair of LC operators handles this. On weekends and holidays, however, only one operator is usually available so the two-person requirement cannot be met and no FIS transfers occur routinely. But if you need a weekend FIS transfer and you are on site, you can telephone the LC operations office (x24531) and then walk down to B-113 to serve as the "second person" yourself.

STEPS:

If you have one or more files you wish to transfer from the Open Environment to the Secure Environment, first gain access to the machine that has the file(s) and position yourself in the directory that contains the file(s). You submit files by using FTP (or SFTP) to make a copy of a file from your local machine onto the transfer machine. Initiate the FTP client software, connect to fis.llnl.gov, and complete the authentication process (by specifying a user name and your current open one-time password). After you have gained access to fis.llnl.gov, change to your TO directory so that you can submit files for transfer. When you use FTP to make a copy from your local machine to the transfer machine you can specify how you want the copy to happen. A binary transfer will copy the file from the local machine to the transfer machine unchanged. In most cases you will want to select the binary transfer mode. The file interchange service treats all files as binary files and does not do any data translation.

You would then proceed to put copies of the local file(s) into the TO directory. Refer to your FTP client documentation for the specific syntax and command usage to perform the above tasks and to determine exactly what functionality is supported by your machine's FTP client software (e.g., "man ftp" on UNIX systems or LC's FTP Manual (URL: http://www.llnl.gov/LCdocs/ftp)). The individual TO directories are scanned periodically and your submitted file(s) are moved to a central collection area. You should not infer that the transfer has been completed by this event. The operators monitor this collection area and depending on the age and amount of accumulated files, they decide to write a transfer tape. They typically will not let a file sit around for longer than two hours before transferring and in general most transfers are completed before the file is even an hour old. Currently, the maximum file size is just under 2 Gbyte for FIS transfers.

This transfer tape is read in on the Secure Environment's transfer machine, nike, and the files are moved to a central distribution area. This central distribution area is scanned periodically and when files exist in

this area, they are distributed to the individual users' FROM directories. The file will have the same name as it had in the TO directory on reebok.

Claiming Open-to-Secure Files

NOTE: FIS does not support file transfers using secure copy (SCP) or NFT; you must use FTP as decribed here. Secure FTP (SFTP) is *not* available on SCF machines.

As a user awaiting the transfer of your file on the Secure Environment's transfer machine, you would optimistically gain access to the machine where you want to use or store the file. In this case you would retrieve files by using FTP to make a copy of a file from the transfer machine onto your local machine. Initiate the FTP client software, connect to fis.scf.cln, and complete the authentication process (by specifying a user name and DCE password). After you have gained access to fis.scf.cln, change to your FROM directory and list the file(s) in the directory. If your file(s) does not exist, then there is a good chance that the operators have not transferred the file(s) yet. The best thing to do is check again after some time has elapsed.

When the file finally appears in the FROM directory, you can then proceed to use FTP to get a copy of the file from the transfer machine and store it on your local machine. As was true above, when you use FTP to make a copy from the transfer machine to your local machine you can specify how you want the copy to happen. A binary transfer will copy the file from the local machine to the transfer machine unchanged. In most cases you will want to select the binary transfer mode. After you have retrieved the files and have stored them on your local machine, you will want to delete the files from the FROM directory. Since the transfer machine has a finite amount of space and transfers will be impacted if file space is critical, it is a good idea to delete the files from the FROM directory once you have retrieved and stored them on your local machine. After several days, files left in the FROM directory will be automatically purged.

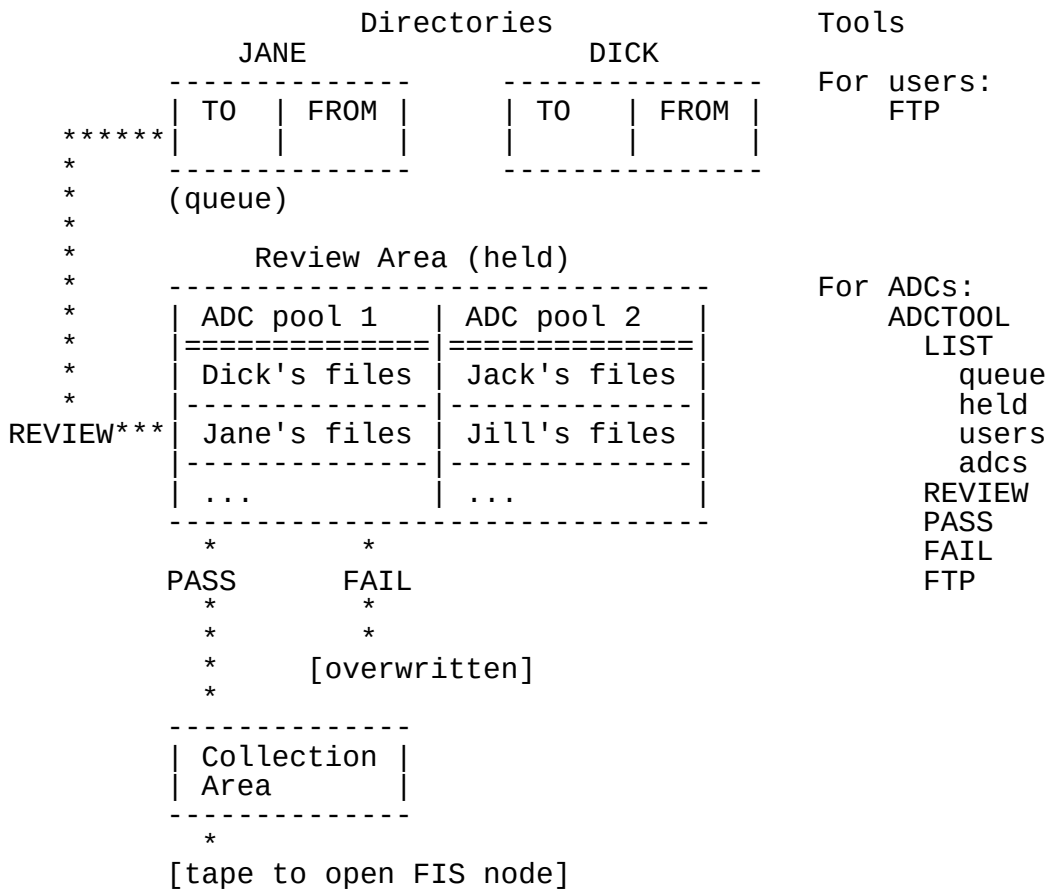
ADC Support for Secure-to-Open Transfers

Review by an Authorized Derivative Classifier (ADC) is part of every secure-to-open FIS file transfer. To help ADCs carry out this review role, FIS provides them a special set of directories dedicated to mananging files undergoing review, and a special software tool (ADCTOOL) for conducting the review online. This section explains both.

Also available to any LC user but especially relevant for ADCs checking multiple text files with possible hidden characters is a MORE-like enhanced file-review utility called MOLE. Other subsections below explain and illustrate how to use MOLE.

ADC Review Area

In addition to the TO and FROM directories seen by each regular user of the secure FIS node, ADCs have access to a separate review area (where files wait hidden from users and protected from outside changes). This review area is organized by ADC pool (next section (page 17)) and by user, and managed when ADCs run the ADCTOOL utility (details below (page 18)). Here is its structure:



ADC Pools

Each organization that partcipates in FIS secure-to-open file transfers has established one or more "ADC review pools" responsible for inspecting candidate files submitted from users in that organization. An ADC review pool consists of one or more ADCs, and follows these rules:

- Each ADC in a pool must be capable of reviewing the content of files submitted by all users assigned to that pool.
- All ADCs in the same pool work as peers, with equal authority. Departments or divisions may, however, add extra security by requiring dual reviews (such as both general and content-specific reviews) from different ADCs for some data.
- Every FIS user is assigned to an ADC review pool based on the scope of their work as determined by their organization.
- A user assigned to one ADC pool can only have their submitted files reviewed by a member of that review pool (although ADCs in the same pool can exchange review duties among themselves to better handle absences or workload).
- An ADC is only permitted to examine and approve (or disapprove) files submitted by the users assigned to his or her review pool.
- Associated with each ADC is a lifetime. Once the lifetime has expired, the ADC cannot access files from their (former) pool for review. The LIST ADCS option of ADCTOOL reveals the current expiration date for every ADC in the pool of the ADC who runs it.

The secure-to-open review process, based on these ADC pools, is simple:

(1) A user submits one or more files for transfer from the secure to the open network (by FTPing them to their TO directory on the secure FIS node).

(2) The user then contacts an ADC from their review pool and alerts them that files await inspection.

(3) The authorized ADC then runs ADCTOOL (next section (page 18)) on the secure FIS node to list the submitting user's queued files, move some (or all) of them to a special area (inaccessible to the user) for formal review, and pass (or fail) the files for transfer once reviewed.

(4) The user learns by checking their README file on the secure FIS node about the outcome of each file review, and claims the file on the open FIS node if it is transferred.

ADCTOOL Explained (ADCs Only)

ADCTOOL Quick Reference Guide

ADCTOOL runs on the secure FIS node and allows Authorized Derivative Classifiers to select, approve, and otherwise manage files that users have submitted for transfer to the open network. ADCTOOL executes as soon as an ADC logs into the secure FIS node (with SSH), offers the prompt

`ADC-`*`yourusername`*`>`

and accepts these commands (as pictured in the diagram (page 16) above):

list [*target*]

reports (by default) all files currently submitted for transfer or held for review by the ADC who runs ADCTOOL, or (with target options) selectively reports
only (queue) submitted files,
only (held) review-held files,
only (users) the users for whom this ADC can perform reviews, or
only (adcs) this ADC's peer reviewers and their expiration dates.

review [*username [filelist]*]

moves the specified file(s) for the specified user into the review area of the ADC who runs ADCTOOL (and, without arguments, prompts for input).

pass [*username [filelist]*]

approves the specified file(s) for the specified user, prompts for a description of the file type(s), moves the file(s) into the collection area for tape transfer to the open network, alerts the user by appending a message to their README file (and, without arguments, prompts for input).

fail [*username [filelist]*]

disapproves the specified file(s) for the specified user, deletes the file(s) and overwrites the space, alerts the user by appending a message to their README file (and, without arguments, prompts for input).

assume [*username [adcname]*]

enables the ADC running ADCTOOL to "assume" review duties from the specified ADC (adcname) for all currently held files of the specified user (and, without arguments, prompts for input).

ftp [*username*]

starts an FTP session so you can move any currently held files for the specified user to another machine where you can examine their contents to determine their classification status (and, without arguments, prompts for input).

help [*command*]

displays general ADCTOOL help, or help on the specified command.

quit ends ADCTOOL and logs out of the secure FIS node.

ADCTOOL Commands (By Function)

If you are an Authorized Derivative Classifier, you can log into the secure FIS node (using SSH) to manipulate files that users have submitted for review. A utility called ADCTOOL runs as a shell as as soon as you log in and offers commands designed to select and (dis)approve user-submitted files, and otherwise share ADC duties among those in your ADC pool.

For a diagram of the relations among the directories and files for review, and the ADCTOOL commands that affect them, see the ADC Review Area section above (page 16). For a brief comparative summary of the ADCTOOL commands, see the preceding section, called ADCTOOL Quick Reference Guide (page 18). The rest of this section gives full technical details on the ADCTOOL commands, grouped by function.

File-Review Commands:

list [queue | held | both [*username*]]
list [*poolname* | adcs | users]

reports the names of available files on the secure FIS node that meet various criteria that you specify, or lists the users or ADCs in your ADC pool if requested. The alternative arguments for LIST are (where *username* and *poolname* are variables and all the other options are literals):

queue [*username*]	lists all files currently in the submission (TO) directory of the specified user, or, without *username*, lists all files in the submission (TO) directories of all FIS users ordered and labeled alphabetically by *username* (users with no files are omitted).
held [*username*]	lists all files that you as ADC are currently holdling in your review area for the specified user, or, without *username*, lists all files held for any user in your review area (users with no files are reported as NONE).
both [*username*]	(default) lists all files currently in the submission (TO) directory of the specified user or held by you as ADC in your review area for the specified user, or, without *username*, lists all files in the submission (TO) directories of all FIS users ordered and labeled alphabetically by *username* (users with no files are omitted) followed by all files held for any user in your review area ordered by user name (users with no files reported as NONE).
[*poolname*]	lists all files currently held in the review area by any member of your ADC pool (useful if you plan to exchange file-review duties).
adcs	lists all ADCs in your pool by user name.
users	lists all users in your pool by user name.

review [*username [filelist]*]

for a specified user (called *username*) who belongs to your ADC review pool, moves all files named in the space-delimited *filelist* from the user's submission (TO) directory into a private (separated by user) review area for your inspection. You (and your peer ADCs, if any) can see such files moved for review, but the submitting user can no longer see or change them. They remain in the user's separate portion of your review area until you pass or fail them (below, usually after you use the FTP option to allow inspection elsewhere). If you specify a *username* but no *filelist*, then all pending files for that user move from the TO directory into the corresponding review area. If you omit both *username* and *filelist*, then ADCTOOL prompts you for the user and then the list of files (and replying with a carriage return selects all pending files for that user).

pass [*username [filelist]*]

for a specified user (called *username*),
(1) prompts you for the "type of data" you are approving (supply any string up to 8 characters, such as ASCII, which will be logged along with each file's name and owner),
(2) declares the file(s) named in the space-delimited *filelist* as unclassified and approved for transfer to the open network,
(3) moves those held file(s) from your ADC review area into the general collection area for tape transfer (and assigns all information needed to deliver each file to the right user on the open FIS node), and
(4) appends to the user's (SCF FIS) README file a message stating that the specified file(s) have passed review.
If you specify a *username* but no *filelist*, then all held files for that user move from the review area into the collection area for transfer. If you omit both *username* and *filelist*, then ADCTOOL prompts you for the user and then the list of files (and replying with a carriage return selects all held files for that user).

fail [*username [filelist]*]

for a specified user (called *username*),
(1) declares the file(s) named in the space-delimited *filelist* as classified and disapproved for transfer to the open network,
(2) removes those held file(s) from your ADC review area and overwrites their disk space to obliterate any possible classified information,
(3) appends to the user's (SCF FIS) README file a message stating that the specified file(s) have failed review.
If you specify a *username* but no *filelist*, then all held files for that user disappear from the review area. If you omit both *username* and *filelist*, then ADCTOOL prompts you for the user and then the list of files (and replying with a carriage return selects all held files for that user). You will see no confirmation of disapproved files.

File-Management Commands:

assume [*username [adcname]*]

enables a second ADC to "assume" review duties from a first ADC (called *adcname*) for all (and only the) currently held (under-review) files submitted by *username*. If one ADC transfers *username*'s file(s) to their review area to begin the classification review, but then does not complete the process (because of a prolonged absence, for example), this command lets any other ADC in the same review pool (only) move the already-held files to their second review area to resume review. If you specify a *username* but no *adcname*, ADCTOOL prompts for the missing ADC's name. If you omit both names, then ADCTOOL prompts for each one.

ftp [*username*]

enables you to move held files to another machine (this is the only way you can examine their content in detail to confirm their classification status). This command:
(1) starts an FTP client on the secure FIS node,
(2) changes local directories so that (only) file(s) submitted by *username* are available for transfer,
(3) lets you OPEN a connection to another secure machine, PUT files, and then QUIT the FTP session,
(4) resumes your ADCTOOL session when FTP ends.
While FTP runs you get its prompt directly (and you can use any of its options). If you omit *username*, ADCTOOL prompts for it. Only a copy transfers to the remote machine; each file's reference version remains in the FIS node's review area until you pass or fail it with ADCTOOL.

Housekeeping Commands:

help [*command*]

displays a brief descriptive list of available ADCTOOL commands, or, if you specify a command name, provides a brief explanation of that command's role.

quit ends ADCTOOL and logs you out of your current interactive session on the secure FIS node.

MOLE (File Review Tool)

MOLE and MORE Compared

MOLE is a MORE-like text-display utility available to all users on all LC production machines (and LC Suns), but customized to help Authorized Derivative Classifiers (ADCs) efficiently and reliably review text files proposed for secure-to-open transfer with FIS.

MOLE and MORE are alike in that both programs:

- display text (ASCII) files at a controlled rate for review (not editing),
- offer a small command set requiring no carriage return to execute the commands once entered (except for requesting a specific line),
- use NOECHO mode so that file output is not interrupted by display of the commands that you type (again, except for requesting a specific line), and
- accept space-delimited lists of files or standard UNIX file filters to display multiple files (one at a time).

MOLE also offers several ADC-relevant enhancements not supported by MORE:

- CONTROL.
  Added MOLE commands enable forward *and backward* movement within each displayed file as well as among multiple files. You can also jump to a specified line number in either direction.
- STATUS INFORMATION.
  MOLE reports features of the file being displayed at the start of each new file (in a header) and at the bottom of each screen (in a prompt); see the next section (page 25) for details.
- NONSTANDARD CHARACTERS.
  In files with fewer that 1% nonASCII characters, MOLE counts and signals each one (with the bell). In files with greater than 1% nonASCII characters (various binary files), MOLE detects and reports their nontext status without trying to display them. MOLE also counts and displays all "hidden" text lines (see next subsection (page 25)).

The table below itemizes the commands and file-management features of MOLE, and compares each with MORE to clarify its significance. The next subsection explains MOLE's prompt and header, and illustrates its behavior.

Feature Comparison of MOLE and MORE for Reviewing Files.

Features	**MORE**	**MOLE**
Shared Commands:		
Display next line	RETURN	RETURN
Display next screen	SPACE	SPACE
Toggle to display half screen (20 lines)	CTRL-D (Sun)	*
Display brief help	?	?
Quit	q	q
Added Commands:		
Display previous screen (or half screen)		L
Display the line numbered *nnn* and the screen (or half screen) of previous lines		*nnn*RETURN
Display the previous file (again)		-
Display the next file (listed on execute line)		+
File Management:		
Prompt for command	Shows percentage displayed so far	Shows MOLE's 9 commands
Status report	Same as prompt	Summarizes file features at (1) start of each file (full), (2) end of each screen (short)
Nonprinting ASCII characters	Pauses at CTRL-L	Ignores, no display
Isolated nonASCII characters	Ignores, no display	Counts, reports, signals each with bell
Whole nonASCII files	Tries to display, grotesque output	Detects, reports, no display
Hidden text lines	Ignores, no display	Counts, reports, displays, signals each with bell
Multiple input files	Displayed in sequence with single-line identifier	File name reported on every screen, forward and back commands

Annotated MOLE Example

Unlike MORE, MOLE reports helpful information about the file that it is being used to review both in (1) a prompt at the end of each screen displayed and (2) a header at the start of each new file displayed. Both MOLE's prompt and its file header need some interpretation, however.

Interpreting MOLE's Prompt.
MOLE's bottom-of-screen prompt has the form

```
? l/f space L # + - * Q   ***  nnnn/k filename  ***
|_____________________|        |_____________|
MOLE commands summarized        status report
```

where the status report (right side) contains:

nnnn is the line number of the line currently displayed just above the prompt (increments as you step through the file).

k is either of two values:
* (if you have reached the end of the file),
A (for an ASCII file not yet ended).

filename is the name of the file currently opened with MOLE (helpful if you are reviewing many files in sequence).

Interpreting MOLE's File Header.
MOLE begins the display of each file with a single-line header of the form

```
[filename]: nnnnL/ccccc revdate  *** mm hidden lines ***
```

where

filename is the name of the file currently opened with MOLE (helpful if you are reviewing many files in sequence).

nnnn is the total number of lines in the file, including hidden lines (if any).

ccccc is the total number of characters (bytes) in the file, including hidden lines (if any).

revdate is the date (and time) when this file was created or last revised (probably quite different than the date when you opened it with MOLE).

mm is the total number of hidden lines found by MOLE when it opened and checked this file (if none, this portion of the header disappears). A hidden line ends with a carriage return without a line feed, so that other lines hide it when the file is displayed by most UNIX editing or output programs (such as MORE). MOLE displays hidden lines in their appropriate place in the file and signals each with the bell.

Example MOLE Session.

```
User: mole test1 test2                                  [open two files]
Rtne: [test1]: 408L/21957 Jan 5, 1998 11:03             [MOLE's header]
      ...first 40 lines of test1 displayed here...      [text]
      ? l/f space L # + - * Q  *** 40/A test1 ***       [MOLE's prompt]
User: *                                                 [toggle to
                                                         20-line display]
Rtne: [bell]                                            [MOLE acknowledges]
User: [space]                                           [request next screen]
Rtne:
      ...next 20 lines of test1 displayed here...       [text]
      ? l/f space L # + - * Q  *** 60/A test1 ***       [MOLE's prompt]
User: [space]                                           [request next screen]
Rtne:
      ...next 20 lines of test1 displayed here...       [text]
      ? l/f space L # + - * Q  *** 80/A test1 ***       [MOLE's prompt]
User: L                                                 [request previous scr]
Rtne:
      ...previous 20 lines of test1 displayed (again)...
      ? l/f space L # + - * Q  *** 60/A test1 ***       [line count
                                                       decremented]


User: 400RETURN                                         [request line 400]
Rtne:
      ...20 lines of test1 ending at line 400...
      ? l/f space L # + - * Q  *** 400/A test1 ***      [note new
                                                       location]
User: RETURN                                            [step forward 1 line]
Rtne:
      ...line 401 added at bottom of screen...
      ? l/f space L # + - * Q  *** 401/A test1 ***      [note new
                                                       location]
User: +                                                 [request next file]
Rtne: [test2]: 110L/5331 Apr 9, 2001 3:17 *** 8 hidden lines***
                                                        [MOLE's header]
      ...first 20 lines of test2 displayed here,        [text]
      including any hidden lines in this range...
      ? l/f space L # + - * Q  *** 20/A test2 ***       [MOLE's prompt]
User: RETURN                                            [step forward 1 line]
Rtne:
      ...line 21 added at bottom of screen...
      ? l/f space L # + - * Q  *** 21/A test2 ***       [note new
                                                       location]
User: -                                                 [request prev. file]
Rtne: [test1]: 408L/21957 Jan 5, 1998 11:03             [test1 redisplayed]
      ...first 20 lines of test1 displayed again...
      ? l/f space L # + - * Q  *** 20/A test1 ***       [MOLE's prompt]
User: q                                                 [quit MOLE]
Rtne: [2 ASCII files reviewed]                          [final status report]
```

Examples

Here are typical file-transfer sessions using LC's File Interchange Service, annotated for analysis.

GOAL: From an open machine, to transfer three files to the secure network using FIS, then retrieve them (2 hours later) on a secure machine.

STRATEGY: User ELVIS...
(1) Runs FTP and connects to FIS.LLNL.GOV (REEBOK),
(2) Confirms that /users/elvis is the arrival directory, with children TO and FROM, and moves into the TO directory,
(3) Requests binary FTP transfer (FIS tapes are always binary), and PUTs three files into /user/elvis/TO,
(4) Ends FTP on the open side.
Two hours later, ELVIS logs on to some SCF machine and then:
(5) Runs FTP and connects to FIS.SCF.CLN (NIKE),
(6) Moves to directory /users/elvis/FROM, and
(7) MGETs the three transferred files as desired.

```
$ ftp fis.llnl.gov ---(1)
Connected to fis.llnl.gov
220-NOTICE TO USERS
[20-line standard security message here]
220-
220 reebok.llnl.gov FTP server (Version...)ready.
202 Command not implemented
Name (fis:elvis): elvis
331 Password required for elvis.
Password: [use your one-time authenticator-generated password]
230 User elvis logged in.
ftp> pwd ---(2)
257 "/users/elvis" is current directory.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (...) (0 bytes)
total 2
FROM
TO
226 ASCII Transfer complete.
ftp> cd TO
250 CWD command successful.
ftp> binary ---(3)
```

200 Type set to I.
ftp> put bubblesort bubble.0301
200 PORT command successful.
150 Binary data connection for bubble.0301 (...).
226 Binary Transfer complete.
45231 bytes sent in ... seconds (... Kbytes/s)
ftp> prompt
Interactive mode off.
ftp> lcd graceland
Local directory now /u0/elvis/graceland
ftp> mput jan feb
local: jan remote: jan
200 PORT command successful.
150 Binary data connection for jan (...)
226 Binary transfer complete.
245212 bytes sent in ... seconds (... Kbytes/s)
local: feb remote: feb
200 PORT command successful.
150 Binary data connection for feb (...)
226 Binary transfer complete.
300975 bytes sent in ... seconds (... Kbytes/s)
ftp> ls -l
200 PORT command successful.
150 ASCII data connection for /bin/ls (...) (0 bytes)
total ...
-rw------- 1 elvis 45232 Mar 01 11:01 bubble.0301
-rw------- 1 elvis 300975 Mar 01 11:02 feb
-rw------- 1 elvis 245212 Mar 01 11:02 jan
226 ASCII Transfer complete.
ftp> quit ---(4)
221 Goodbye.
[...2 hours later on the secure network...]
$ ftp fis.scf.cln ---(5)
Connected to nike.scf.cln
220-NOTICE TO USERS
[20-line standard security message here]
220-
220 nike.scf.cln FTP server (Version...) ready.
202 Command not implemented
Name (fis:elvis): elvis
331 Password required for elvis.

```
Password: [use your secure DCE password]
230 User elvis logged in.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (...) (0 bytes)
total ...
FROM
TO
226 ASCII Transfer complete.
ftp> cd FROM ---(6)
250 CWD command successful.
ftp> binary
200 Type set to I.
ftp> prompt
Interactive mode off.
ftp> pwd
257 "/users/elvis/FROM" is current directory.
ftp> ls -l
200 PORT command successful.
150 ASCII data connection for /bin/ls (...) (0 bytes)
total ...
-rw------- 1 elvis 45232 Mar 01 13:01 bubble.0301
-rw------- 1 elvis 300975 Mar 01 13:02 feb
-rw------- 1 elvis 245212 Mar 01 13:02 jan
226 ASCII Transfer complete.
ftp> mget jan feb bubble.0301 ---(7)
local: jan remote: jan
200 PORT command successful.
150 Binary data connection for jan (...).
226 Binary Transfer complete.
224598 bytes sent in ... seconds (... Kbytes/s)
local: feb remote: feb
200 PORT command successful.
150 Binary data connection for feb (...).
226 Binary Transfer complete.
220541 bytes sent in ... seconds (... Kbytes/s)
local: bubble.0301 remote: bubble.0301
200 PORT command successful.
150 Binary data connection for bubble.0301 (...).
226 Binary Transfer complete.
193456 bytes sent in ... seconds (... Kbytes/s)
```

```
ftp> bye
221 Goodbye.
```

Limits

This section summarizes the technical limitations of FIS file transfers.

Maximum number of files at once: none
(but use TAR to combine many small, related files for better service).

Maximum file size: 2 Gbyte minus 100 bytes
(files near the maximum size will usually transfer much more slowly than normal, up to several hours).

Maximum disk capacity (on each FIS node): 36 Gbyte

Maximum number of simultaneous FIS users: 25 (with FTP, no limit with SFTP)

File name characters: see "How FIS Handles File Names," above (page 12), for FIS character mappings and a work-around.

Disclaimer

Keyword Index

To see an alphabetical list of keywords for this document, consult the next section (page 35).

Keyword	Description
entire	This entire document.
title	The name of this document.
scope	Topics covered in FIS Manual.
availability	Where FIS is available.
who	Who to contact for assistance.
introduction	Role and goals of FIS.
overview	FIS features diagramed, summarized.
fis-form	How to get FIS passwords, rules.
fis-authorization	Requesting FIS authorization.
passwords	Password policies on open, secure sides.
authorization-levels	Classification review categories.
deny	No secure-to-open transfers.
need	Secure-to-open with ADC review.
dusa	This category has been suspended.
admin	This category has been suspended.
usage	How to use FIS.
file-names	How FIS handles unusual characters.
deposit	Depositing open-to-secure files.
claim	Claiming open-to-secure files.
adc-support	Rules, tools for secure-to-open transfers.
adc-diagram	Diagram of ADC review area and its use.
adc-pools	How review pools work for users and ADCs.
adctool	Software tool for secure-to-open transfers.
adctool-guide	ADCTOOL quick reference guide.
adctool-commands	ADCTOOL options thoroughly explained.
mole	Enhanced file-review tool.
mole-features	How MOLE and MORE features compare.
mole-example	MOLE's prompt, header, sample output.
examples	Typical annotated FIS sessions.
limits	FIS limitations summarized.

index	The structural index of keywords.
a	The alphabetical index of keywords.
date	The latest changes to FIS Manual.
revisions	The complete revision history.

Alphabetical List of Keywords

Keyword	Description
a	The alphabetical index of keywords.
adc-diagram	Diagram of ADC review area and its use.
adc-pools	How review pools work for users and ADCs.
adc-support	Rules, tools for secure-to-open transfers.
adctool	Software tool for secure-to-open transfers.
adctool-commands	ADCTOOL options thoroughly explained.
adctool-guide	ADCTOOL quick reference guide.
admin	This category has been suspended.
authorization-levels	Classification review categories.
availability	Where FIS is available.
claim	Claiming open-to-secure files.
date	The latest changes to FIS Manual.
deny	No secure-to-open transfers.
deposit	Depositing open-to-secure files.
dusa	This category has been suspended.
entire	This entire document.
examples	Typical annotated FIS sessions.
file-names	How FIS handles unusual characters.
fis-authorization	Requesting FIS authorization.
fis-form	How to get FIS passwords, rules.
index	The structural index of keywords.
introduction	Role and goals of FIS.
limits	FIS limitations summarized.
mole	Enhanced file-review tool.
mole-features	How MOLE and MORE features compare.
mole-example	MOLE's prompt, header, sample output.
need	Secure-to-open with ADC review.
overview	FIS features diagramed, summarized.
passwords	Password policies on open, secure sides.
revisions	The complete revision history.
scope	Topics covered in FIS Manual.
title	The name of this document.
usage	How to use FIS.
who	Who to contact for assistance.

Date and Revisions

Revision Date	Keyword Affected	Description of Change
03Mar03	overview	Two-person rule, weekend work-around.
	deposit	Two-person rule, weekend work-around.
10Feb03	overview	SFTP role, features noted.
	passwords	SFTP offers DSA key authentication.
	deposit	SFTP access added.
	limits	SFTP limits noted too.
05Sep02	overview	Maximum capacity vs. per-file limit.
	limits	Maximum capacity vs. per-file limit.
	passwords	OTP required for open FIS now.
09Oct01	overview	Open OTP for FIS ok.
	passwords	Open OTP for FIS ok.
	deposit	Open OTP for FIS ok.
	examples	Dialog updated for passwords.
25Jul01	overview	NIKE, REEBOK names deemphasized.
	usage	NIKE, REEBOK names deemphasized.
	examples	Minor technical corrections.
15May01	mole	New section on new ACD tool.
	introduction	Cross ref to MOLE added.
	index	New keywords for new subsections.
22Jan01	file-names	New section on special characters.
	overview	Warning on special characters.
	limits	Cross ref to new section added.
	index	New keyword for new section.
16Nov00	need	Dual ADC reviews may be needed.
	adc-pools	Dual ADC reviews may be needed.
04Oct00	overview	Max 25 simultaneous FIS sessions.
	usage	Max 25 simultaneous FIS sessions.
05Jun00	introduction	Document scope expanded for ADCs.
	adc-support	New section on secure-to-open transfers.
	overview	FTP gateway eliminated.
	usage	README role clarified.
	authorization-levels	Only NEED and DENY in operation.
	index	New keywords added.
03Jan00	limits	New summary section added.
	index	New keyword added.
09Sep99	overview	New FIS nodes, file size.
	passwords	FIS uses DCE passwords now.
	usage	DCE passwords, new node names.
	examples	Security waring, other details updated.

15Jun99	introduction	Cross ref. to EZOUTPUT expanded.
	deposit	Warning about Macintosh file names.
04Jun99	passwords	Telnet for password change restricted.
	deposit	FTP firewall warning cross referenced.
06Apr99	overview	Firewall now blocks outside access.
09Mar99	overview	Firewall alert, SCP warning added.
	passwords	Kerberos use clarified.
	usage	SCP warnings added.
	who	New area code, SCF e-mail.
19Feb97	overview	OCF drops from HOPPER's
	passwords	domain name on open net.
	deposit	IP address changed too.
	examples	
06Jan97	entire	First edition of LC FIS Manual.

TRG (03Mar03)

UCRL-WEB-201520

TRG (03Mar03) Contact on the OCF: lc-hotline@llnl.gov, on the SCF: lc-hotline@pop.llnl.gov